BRANDLE

The Hidden Security Risks from the Corporate Social Media Footprint

Why You Should Be Concerned About Your Shadow Network of Connected applications

SOCIAL MEDIA GOVERNANCE

The Hidden Security Risks from the Corporate Social Media Footprint

Why you should be concerned about your shadow network of connected applications

By Chip Roberson, CEO, Brandle, Inc.

Introduction

A universe of applications, many hidden from view, are connected to your corporate social media properties. Uncounted, unmonitored, and ungoverned, each is a potential risk to your enterprise.

Think about the many social media properties, which represent your enterprise, and ask yourself:

- Over time, how many people have had the ability to connect applications?
- How many people still have the credentials or permission to connect applications?
- How many applications now have access to these properties?
- Have any of those applications been compromised?
- Have any of the credentials used to log into those third-party applications been compromised?

These are the questions that every corporate Security and Social Media Governance professional should be asking. This whitepaper highlights key data that shows the prevalence of the hidden security risks from the corporate social media footprint.

Numerous Attack Vectors

Consider these two examples: the author discovered 31 applications/websites connected to his Twitter account; Brandle's corporate Twitter account had 20 connections. These connections include other social platforms, publishing apps, customer support systems, sharing tools, customer relationship systems, and a host of websites that use social sign-on.

The connection of unauthorized or uncontrolled applications (i.e. "shadow IT") to corporate social media properties is a significant, persistent, and on-going risk to any enterprise. Social media arose in a "wild west" environment, where accounts were created and managed without any form of structure or governance. This means that every enterprise has a vast array of properties on numerous social media platforms with no record of the applications which have access to them.

Any of these "invisible" applications could be an attack vector to your company, compromising your brand, creating a security vulnerability, or be the source of a post meant to manipulate public markets. Every application connected to a social media property is another doorway to your online presence. Some of these applications are from well-established businesses with solid security. However, we all know that random applications have been given access in order to perform some special action like auto-follow, auto-reply, schedule future posts, get analytics, social sign-on, etc. Even if the service itself has not been compromised, each connected application could represent another set of credentials which themselves may have been compromised.

While some enterprises have taken notable steps to "lock down" access to their social media, even the best enterprises still have unauthorized applications connected to their properties. Unfortunately, the social media platforms do not make it easy to audit which applications have access to which property, especially across a large inventory. This lack of support for social media governance is a major failing of the platforms, which puts their customers, their users, and the general public at risk.

This problem is further exacerbated by the fact that most enterprises do not have a complete and accurate inventory of every social media property its employees and agents, past and present, have created to represent it.

In the discussion below, you will see the reference to "POPs" or "points-of-presence." This is a term we use as a catch-all for the various forms for presence on the web, such as Twitter accounts, Facebook pages or groups, YouTube channels, Pinterest boards, etc. All are points-of-presence, which represent some aspect of the enterprise.

What We Found

Fortunately, three platforms (Facebook, Twitter, and LinkedIn) provide some data about the source of a published post. Recently, Brandle added the POP Post Governance feature to the Brandle Presence Manager, which gives companies a pan-enterprise view of:

- Which publishing applications have been used to post content;
- Which POPs are the recipients of a publishing application's posts;
- Which publishing applications are posting to a given POP.

While this does not provide a complete picture, as there could be other applications sitting silently awaiting the right time to strike; it does, however, provide a good starting place to reduce the number of vectors by which your enterprise could be attacked.

We have used POP Post Governance to assemble an aggregated view of what our customers are seeing to highlight the magnitude of this risk. Below is a summary of what we found.

Please note that this analysis is on a subset of our customers, selected to be a representative sample of enterprises using the Brandle Presence Manager to protect their owned properties. Therefore, we limited the analysis to enterprises which did not contain the POPs of employees (e.g. sales agents, ambassador programs, etc). The companies

are generally quite large and diverse with business classifications that include banking, conglomerates, express logistics, financial services, medical equipment, and pharmaceuticals.

We did not include retail enterprises in this analysis due to the fact that they may employ a more liberal (and more distributed) governance strategy regarding their social media properties and tools than the other companies in this study.

What is a Publisher?

For the purpose of the study, a "publisher" is any application, which is the source of a post to an enterprise's POP. Therefore, any application which has the ability to post content may be considered a "publisher" for the purposes of this analysis.

Publisher Counts

The first question we wanted to know was: ***How many publisher applications are we detecting for these enterprises?*** A well-governed enterprise should have fewer applications than one which is not.

The median number of publisher applications per company is 11 (mean=12.5). The max is 23. In other words: The average enterprise has 11 publisher applications actively posting to their points-of-presence, the largest has 23.

Analysis: Given that we are only examining the publishers for just three platforms (Facebook, Twitter, and LinkedIn) and that one of those platforms (LinkedIn) is published to less frequently and does not always report the source of the post, one could loosely interpret this as "eleven (11) applications posting to two (2) platforms." If an enterprise has standardized on a single publisher (e.g. Khoros Social, Sprinklr, or Hootsuite) and they have restricted their employees, contractors, and agencies from having "native" access to a POP, we would expect this number to be closer to 3-4 publishers per platform; for

example: a social media management system, a chatbot/support app, and perhaps an outside agency app.

Thus ideally, for these three (3) platforms combined, we would like to see the Publisher Count be closer to 9 (e.g. one SMMS, one chatbot, and one other app per platform) and certainly not up around 23. The fact that the median and mean were 11-12 and the max was 23 indicates there is room for improvement here.

POP Counts

To put the Publisher counts into perspective, it is important to have an idea of the number of POPs to which these applications may be publishing. Again, these are just the number of Facebook, Twitter, and LinkedIn POPs in each account; not the total size of their inventory across all platforms.

The median account had 926.5 POPs (mean=944), while the minimum was 185 and the max was 1,719. It is worth noting, however, that we have other accounts (e.g. retail) not included in this study with many more than 1,719 POPs on these three platforms.

Looking at one account, which has close to the average number of POPs, we see the following relative number of POPs by platform:

- 9.1x more POPs on Facebook than LinkedIn
- 4.3x more POPs on Twitter than LinkedIn
- 2.1x more POPs on Facebook than Twitter

These ratios will be useful when we look at the most frequently used publishing apps below.

Publisher-to-POP Ratio

To put the Publisher Counts into perspective, we compared each count to the POP Count for each respective enterprise. We calculated the Publisher-to-POP Ratio by dividing Publisher Count by the POP Count, normalized by 1,000:

Publisher-to-POP Ratio = Publisher Count ÷ (POP Count ÷ 1,000)

The median ratio of publishing applications per 1,000 POPs was 11.5 (mean=13.3). The minimum was 5 and the maximum was 29.

Analysis: The thinking here is that the larger the inventory, the more likely there may be segmentations by geography, business unit or line, language, etc., which results in more publishing applications being employed. For example, Asia may have standardized on a different set of tools than North America or Europe. However, in the Most Used Publishers section below, we will see that size of the inventory is not the most significant factor affecting proliferation of publishing applications.

Note: the max Publisher-to-POP Ratio of 29 is larger than the max Publisher Count of 23. This is a result of the POP Count for this particular enterprise being below 1,000 and thus we are dividing 23 by a number that is less than 1.0. In other words, when factoring in the size of the inventory, this particular enterprise, which was already an outlier, looks even worse.

POP Publisher Count

The next question we want to answer was: ***How many publishers are there for each POP?***

Here the numbers are better, the median number of publishers per POP is 1.0, while the mean=1.27. The maximum we found was 4 publishers per POP.

Analysis: Given that we recommend no more than 3-4 publishers per POP, the fact that we see a mean and median less than 2 and a maximum of 4 is indicative that no one has gone crazy in attaching too many active publishers to a single POP. However, this does indicate that individuals within the enterprise are likely connecting different publishing apps to their platforms (see below) and thus a lack of adherence to standards.

Publisher POP Counts

Conversely, we wanted to know: *To how many POPs is each application publishing? Are we seeing a lot of applications posting to just a few POPs or vice-versa?*

What we found was that the median application published to just 1 POP, while the mean was larger at 6.23 POPs per application. The maximum number of POPs to which an application is publishing is 112.

Analysis: A median value of 1 tells us that there is a significant number of "one offs," where someone has attached a favorite tool to just one POP. Additionally, a mean of 6.23 and a maximum of 112 indicates two things: a) there is some progress towards standardization but b) given the size (and relative size) of the POP inventories, that standardization is not comprehensive. This reinforces the analysis above for the POP Publisher Count.

Most Used Publishers

As a final look at the data, we wanted to answer: *What publishing applications were most used, across all enterprises?*

Below is a list of the top ten (10) publishers based on the number of posts made by those applications. Rather than displaying the absolute number of posts, we normalized the values relative to the most frequently used application -- Khoros Social Marketing for Facebook. This gives one a sense of their relative use. For example, Coversocial is being used to make 59% as many posts as Khoros Social Marketing.

Khoros Social Marketing	Facebook	1.00
Conversocial	Twitter	0.59
Twitter Web App	Twitter	0.59
Service App	Twitter	0.24
Hootsuite Inc.	Twitter	0.24
Twitter for iPhone	Twitter	0.18
OBI4wan	Twitter	0.17
Khoros	Twitter	0.16
Twitter for Advertisers	Twitter	0.15
Twitter for Android	Twitter	0.15

Analysis: A few details jump out based on this table.

First, Khoros is definitely the most used application for the customers sampled for this study. While Sprinklr is in this customer set, it appears further down and only for Twitter. We cannot rule out that this could be the result of a) the customers who choose to use the Brandle Presence Manager and b) the customers who were selected to be in this study. Khoros and Sprinklr are the two most mentioned social media management systems (SMMS) by our customers, followed by Hootsuite, Sprout Social, and Salesforce (appearing further down in the data). Note: it is not uncommon for the same application to have different names on different platforms: we see "Khoros Social Marketing" for Facebook but just "Khoros" for Twitter; similarly we see "Salesforce Marketing Cloud" for Facebook but "Salesforce - Social Studio" for Twitter, which is part of the Salesforce Marketing Cloud.

Second, the fact that Facebook appears just once and at the top, while Twitter fills the other nine (9) spots may be attributable to a fundamental difference in how those two platforms approach access. Facebook is a "permission-based" platform, where individuals

cannot log directly into a POP (e.g. a Facebook Page) but are given access, which may be revoked at any time. Twitter, on the other hand, is a "credential-based" platform, where each POP has its own ID and password. Thus, anyone with the Twitter password can log into the account and connect (OAuth) a third-party application to that POP. This is why we see Twitter Web App, Twitter for iPhone, Twitter for Android, occupy 30% of the top 10 (as well as Twitter for iPad, which did not make the top 10). The implication is that a permission-based platform is much more secure than a credential-based one precisely because there is no password to pass around and access can be revoked on an individual basis (without affecting everyone else and every other connected application).

Third, Twitter is often the platform of choice for requesting support or lodging a complaint with a company. This may increase the number of support tools, which may be attached to a POP to allow for automated and human responses to those support requests. This can explain the appearance of Conversocial and Service App (by Novomind) in the top 10.

Conclusions

Here are some of the conclusions we take away from this analysis.

Platform utilization affects connected applications

The area of largest concern is obviously the number of publishing apps connected to POPs on the Twitter platform. While some of this difference between Facebook and Twitter can be attributed to the nature in which they are used by the general public, we conclude that it does not account for the bulk of what we observed.

Signs of compliance, possibly thanks to permission-based access

We see signs that some team members are complying with company policies and using authorized publishing applications but it is not widespread. While governance practices appear to be most successful on Facebook, likely due to their permission-based access structure, the process is not complete and governance of Twitter POPs appears to be

lagging. It is worth noting here that there are other platforms, like Instagram, Pinterest, and Snapchat, which are also credential-based but were not part of this study.

Twitter, while less prevalent, appears to pose greatest risk

The problem with POPs on the Twitter platform is exacerbated by the fact that customers generally have half the number of POPs on that platform as compared to Facebook. In other words, relative to Facebook, Twitter has 9 times the number of publishing applications for half the number of POPs.

Additionally, as we have seen in recent social media hacks, Twitter appears to be the vector of choice and with the potential to have significant, possibly global (e.g. market moving), impact. However, it should be noted that much of what happens on Facebook could be out of view of the general public. Twitter may appear more vulnerable simply because posts on Twitter are much more public.

Lack of visibility leaves companies vulnerable

Any application that is connected to a social media point-of-presence for an enterprise is vulnerable to hacking, which we saw earlier this year. If an enterprise has an ad hoc collection of applications or accounts on those applications connected to their global presence, it may not know which of their properties are at risk and thus require immediate action.

Access Audits are not (easily) supported by all platforms

Something not directly addressed above is the ability to see what applications are connected to your POP. While we called out Twitter for its lack of a permission-based access mechanism, this is one area where Twitter gets higher marks than Facebook. From the Settings > Applications screen (https://twitter.com/settings/applications), one can see all of the applications which have been connected to a Twitter account. However, while Facebook offers that feature for their user accounts (https://www.facebook.com/settings?tab=applications), a similar capability is reported to

exist for their pages but the author has yet to find it after several extensive searches. While access to a user account, which may have certain rights to a page, is important, a company should be able to see what applications have access to their pages.

Recommendations

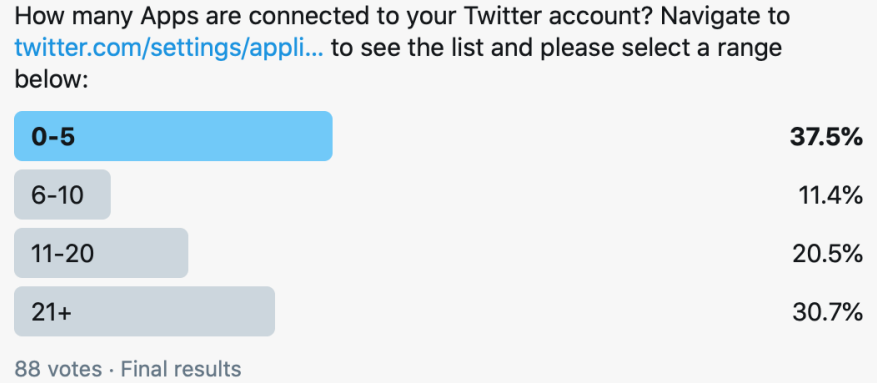
We offer the following recommendations:

1. Continue bringing Facebook POPs under a small set of authorized applications (e.g. Khoros, Sprinklr, Hootsuite, Salesforce, etc).
2. Acquire and centralize the passwords for all Twitter accounts (as well as for Instagram, Pinterest, Snapchat, etc.) in a single password management system, which can provide a permission-based access to these platforms.
3. Once the password has been acquired, change it so no unauthorized person can log into the account.
4. Additionally, once control of the account is acquired, ensure that no personal email accounts are used as a credential or recovery email for the POP. Any email address associated with a corporate property should be hosted on the corporate domain and/or under corporate control. Ideally, the email account should be based on a role, not a particular person (e.g.: sm_mgr_europe@company.com rather than jane.smith@company.com or worse yet, john.smith@gmail.com). Note: Twitter does not allow the same email address to be used on more than one account. Ask your mail administrator if your company has the ability to create aliases like Gmail's task specific email addresses: m_mgr_europe+brand1@company.com, m_mgr_europe+brand2@company.com, etc. This will allow one email account to serve multiple Twitter accounts. See: https://support.google.com/a/users/answer/9308648?hl=en.
5. Remove access (OAuth) to any applications not approved by the enterprise, especially any which are unrecognized.
6. Similarly, for any third-party applications which are required by your enterprise but are credential-based, like bit.ly, similarly collect and protect the credentials.

7. Monitor the list of applications, which are publishing to your POPs (e.g. with a system like the Brandle Presence Manager).
8. Perform periodic audits of your POPs to review who has access and what applications have been authorized (OAuth) to access them. Some platforms make this easier than others.
9. Petition your account managers at the various platforms to make governance a priority and to allow authorized applications (like the Brandle Presence Manager) to monitor all applications connected to your POPS, not just those publishing content, on your behalf.
10. In lieu of Platform API support to monitor connected applications, enterprises should perform periodic "access audits" of their social media POPs. Each connected application, whether for publishing, listening, engagement, etc., should be evaluated and removed if access is no longer required. The connected applications which remain should be documented for each POP in a central inventory system, like the Brandle Presence Manager, for quick identification and action should a crisis arise.
11. Finally, have your employees undertake a similar audit of the applications connected to their personal accounts. Given how social engineering has been used to get past an enterprise's security practices, an app connected to an employee's personal account could be just as dangerous as one connected to a corporate account.
12. Repeat this audit process periodically (e.g. annually or semi-annually).

We hope this analysis is helpful in understanding the risks posed to all enterprises from applications connected to your social media properties, some of which may be lurking the shadows. The moniker "Shadow IT" is very apt in this social media environment. The risks are real and the platforms don't make it easy for enterprises to monitor and address them but there are tools and practices a governance team can employ to decrease these risks and prepare for when, not if, the next crisis arises.

Sidebar: While the adjacent study focuses only on applications that are actively publishing content, the following, albeit non-scientific, survey (n=88) was taken on Twitter to highlight how significant the issue could be. People were asked to count and report the number of applications that they found connected to their personal Twitter accounts. While 37.5% had 5 or fewer connected applications, over 50% found more than 11 and over 30% discovered 21 or more:



It is worth noting that several participants responded privately that the number of applications they found exceeded 50 and one respondent reported over 200! Additionally, many respondents noted finding applications which they no longer recognized or considered necessary. It is safe to say the general response was one of "surprise!" There is no reason to believe that corporate POPs are immune to this accumulation of connected accounts.

Brandle®, Inc, is dedicated to providing a comprehensive system for companies to manage the properties of their brands, identities, and relationships across the web and on all major social networks including Facebook, Twitter, Instagram, YouTube, LinkedIn VK, and more. It is our mission to be the trusted source for social media governance and web presence management and to provide functionality that helps every enterprise manage, secure and protect their brands.

The Brandle® Presence Manager is the foundation of our social media governance and web presence management SaaS. There are three add-on modules: Brand Patrol, GRC (Governance, Risk Management and Compliance), and Ad Accounts.

The data in this whitepaper was collected using our POP Post Governance feature set, which is part of the GRC Module.

If you would like more information about Brandle, review our website at www.brandle.net or contact us via email at info@brandle.net.

Brandle, Inc.

19201 Sonoma Hwy | #381

Sonoma, CA 95476

866-823-4330

www.brandle.net

info@brandle.net